KIRCHER

Group Properties of the Residue Classes of Certain Kronecker Modular Systems and some Related Generalizations in Number Theory

Mathematics

Ph. D.

1914

GROUP PROPERTIES OF THE RESIDUE CLASSES OF CERTAIN KRONECKER MODULAR SYSTEMS AND SOME RELATED GENERALIZATIONS IN NUMBER THEORY

BY

EDWARD AUGUST THEODORE KIRCHER

A.B. University of Illinois, 1911

A.M. University of Illinois, 1912

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

DOCTOR OF PHILOSOPHY

IN MATHEMATICS

IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1914

UNIVERSITY OF ILLINOIS

THE GRADUATE SCHOOL

May 11 1914

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Edward August Theodore Kircher

ENTITLED Group properties of the residue classes of certain Kronecker modular systems and some related generalizations in number theory

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF Doctor of philosophy

G. A. Miller
In Charge of Major Work

E. J. Townsend
Head of Department

Recommendation concurred in:

E. J. Townsend
G. A. Miller
Arnold Emch
Jakob Kunz
F. W. Reed

Committee on Final Examination

TABLE OF CONTENTS.

GROUP PROPERTIES OF THE RESIDUE CLASSES OF CERTAIN KRONECKER MODULAR SYSTEMS AND SOME RELATED GENERALIZATIONS IN NUMBER THEORY.

INTRODUCTION.

The object of this paper is to study the groups formed by the residue classes of a certain type of Kronecker modular systems and some closely related generalizations of wellknown theorems in number theory. The type of modular systems to be studied is of the form $\mathfrak{M}=(\psi,\mathfrak{m})$ where ψ is a rational integral function of x of the form $x^r + a_1x^{r-1} +..+ a_r$, whose exponents are positive rational integers and whose coefficients are algebraic integers of the realm Ω of degree n, while $\mathfrak{m}$ is an ideal belonging to the realm Ω and defined by the fundamental system $(m_1,m_2,...,m_n)$. In a similar manner $(\psi,m_1,m_2,...,m_n)$ shall be said to be the *fundamental system of* $\mathfrak{M}$, so that every expression belonging to $\mathfrak{M}$ can be written as a linear function of the elements comprising this system. In what follows we shall confine ourselves to integers and rational integral functions of x with integral coefficients in Ω, and for the sake of brevity we shall designate as polynomials all such functions of x including those of degree 0. This is equivalent to confining ourselves to the domain of integrity of (Ω,x).

The first part of this paper will be devoted to a historical sketch showing the development of several of the fundamental concepts used together with their necessary definitions. The second part will then be devoted to setting up a necessary and sufficient condition that a set of residue classes belonging to a modular system forms a

group with respect to that system. In the third section the structure of this group will be studied and it will be shown that there exists a simple relation between the factors of the modular system and the generating subgroups of the group belonging to our modular system. The last section will then be devoted to the generalization of a number of well-known theorems of number theory by means of the results of the preceding sections. Theorems 12, 16, 19, and 21, which are here generalized for the realm (Ω, x), have already been extended so as to apply to the realm $(x, 1)$ by Hensel[1] and Landsberg[2].

I. HISTORICAL SKETCH AND DEFINITIONS.

Gauss, the founder of the theory of congruences, has already studied congruences of the form $f_1(x) \equiv f_2(x)$, mod p, where $f_1(x)$ and $f_2(x)$ are rational integral functions of x with rational integral coefficients and p is a rational prime[3]). Probably his most important theorem is that any function of x in the rational realm can be factored in one and only one way into irreducible factors, mod p. Other realms are not considered. This article was not published until after the death of Gauss, so that Schönemann, who seems to have been unaware of this work, carried out some similar investigations[4]). In these he studied the congruence of two functions of x with respect to the modulus (p, α), where p is a rational prime and α a root of the equation

---

1) Hensel, Crelle's Journal, v. 118 (1897), pp. 234-250, v. 119 (1898), pp. 114-130, 175-185.

2) G. Landsberg, Göttinger Nachrichten, 1897, pp. 277ff.

3) Gauss, Werke, Göttingen, 1876, v. 2, pp. 212ff.

4) Schönemann, Crelle's Journal, v. 31 (1846), p. 269; v. 32 (1846), p. 93.

$f(x)=0$ irreducible in the rational realm. He defines the congruence $\psi(\alpha)\equiv\varphi(\alpha)$, mod (p,α), by the equation $\psi(\alpha)=\varphi(\alpha)+p\cdot\theta(\alpha)$, and proceeds to study the congruence $f_1(x)\equiv f_2(x)$, mod (p,α), where all the coefficients of the two functions, let us designate them by ψ's and φ's respectively, are functions of α, coefficients of equal powers being congruent modulo (p,α), so that $\psi_i(\alpha)\equiv\varphi_i(\alpha)$. Dedekind studied some of the properties of the modular system (ψ,p)[5]) where ψ is a rational integral function of x with rational integral coefficients and p is a rational prime. He defines $f_1(x)$ and $f_2(x)$ as congruent modulo (ψ,p) whenever there exists an equation

$$f_1(x) = f_2(x) + \psi(x)\zeta(x) + p\cdot\theta(x),$$

studies those residues of the system that are prime to this modular system, and extends both Fermat's and Wilson's theorem to this case, the latter, however, supposing ψ to be irreducible, mod p. Serret[6]) has also done considerable work along this line for the case when ψ is irreducible, mod p. Among other things he has shown that when this happens all residues excepting the 0 form a cyclic group.

Turning to the single modulus we find that the study of the residue system belonging to such a modulus from the view-point of group theory is almost as old as group theory itself. Cauchy[7]) already studied some properties of such a group, but not much seems to have been done until Tanner studied the group of totitives or residues less than and prime

---

[5]) Dedekind, Crelle's Journal, v.54 (1857), pp. 1-18.

[6]) Serret, Cours d'Algèbre Supérieure, third edition, v.2, §§ 345 & 368. See also Dina, Giornale di Matimatiche, v.21 (1883), pp.234ff.

[7]) Cauchy, Exercises d'Analyse et de Physique Mathématique, 1844, v. 3, pp. 232ff.

to the modulus m, where m is a rational integer[8]). Other papers giving extensive results have been published by Bachmann[9]), Weber[10]), Zsigmondy[11]), and G.A.Miller[12]). Among the theorems stated by the last one of these is the following: All residues of the complete residue system belonging to the modulus m, where m is a rational integer, that have the same greatest common divisor d with m form an abelian group modulo m when and only when they are relatively prime to m/d. This theorem will be generalized in this paper. Ranum[13]) has made a complete study of these groups for the case of a composite ideal modulus m belonging to a quadratic realm, while Wolff[14]) has partly extended this to any realm Ω.

The general concept of a modular system was introduced by Kronecker[15]) and has been considerably extended by Hensel[1]), Landsberg[2]), Moore[16]), König[17]), and others. The following theorem proven by G.A.

[8]) Tanner, Proceedings, London Mathematical Society, v. 20 (1888-9), pp. 63-83.

[9]) Bachmann, Elemente der Zahlentheorie, 1892, p. 57.

[10]) Weber, Algebra, v. 2, 1896, p. 60.

[11]) Zsigmondy, Monatshefte für Mathematik und Physik, v. 7 (1896), pp. 185ff.

[12]) G. A. Miller, Annals of Mathematics, ser. 2, v. 6 (1905), p. 49 (Apr). See also American Journal of Mathematics, v. 27 (1905), pp. 315ff.

[13]) Arthur Ranum, Transactions of the American Mathematical Society, v. 11 (1910), pp. 172-198.

[14]) Georg Wolff, Gruppen der Reste eines beliebigen Moduls im algebraischen Zahlkörper, Diss. Giessen, Göttingen, W. Kaestner, 1905. For the relation of the term "functional" used in this paper with the term ideal see Weber, Algebra, v. 2, 1896, pp. 547ff.

[15]) Kronecker, Vorlesungen über Zahlentheorie, 1901, pp. 146, 158.

[16]) Moore, Bulletin of the American Mathematical Society, ser. 2, v. 3 (1897), p. 372.

[17]) König, Theorie der algebraischen Grössen, pp. 351-361, 401ff.

Miller[18]) has also been generalized in this paper: The group of residues belonging to the modular system (ψ,p) that contains the operator 1, where p is a rational prime and ψ a rational integral function of x with rational integral coefficients, is the direct product of the groups of residues containing 1 of the modular systems (ψ_1,p), (ψ_2,p), ..., (ψ_r,p), where the modular system (ψ,p) is equal to the direct product of the modular systems (ψ_j,p), $j=1,2,...,r$. Finally the modular system (ψ,m) where m is a rational integer and ψ is a rational integral function of x with rational integral coefficients that is irreducible with respect to every rational prime divisor of m taken as a modulus, has been studied by Miss Sanderson[19]).

We shall now give some necessary definitions, and for the sake of brevity shall designate $f(x)$, $\psi(x)$, etc. by f, ψ, etc. Two functions of x, say f_1 and f_2, shall be defined as being *congruent* with respect to the modular system $\mathfrak{M}=(\psi,m)$ when their difference is contained in $\mathfrak{M}$, i.e.

$$f_1 \equiv f_2 \qquad \mod \mathfrak{M},$$

whenever there exists a linear form of the fundamental system of $\mathfrak{M}$ such that

$$f_1 - f_2 = \psi\zeta + m_1\theta_1 + m_2\theta_2 + \dots + m_n\theta_n,$$

ζ and the θ's being polynomials. From this it follows that

$$f_1 - f_2 - \psi\bar{\zeta} \equiv 0 \qquad \mod m,$$

and hence every coefficient of the polynomial obtained by carrying out the operations indicated on the left hand side of the congruence is an integer contained in m. Since any integer in m differs from any other

18) G. A. Miller, Archiv für Mathematik und Physik, v. 15(1909), pp. 115-121

19) Miss Sanderson, Annals of Mathematics, ser. 2, v. 13(1911), pp. 36-39.

integer in m by a linear form of the fundamental system of m, it follows that by adding the proper linear form to each coefficient of the polynomial $f_1-f_2-\psi\zeta$, which is equivalent to adding to this polynomial itself a linear form in m, we can make every coefficient of this polynomial divisible by any integer contained in m. All congruent polynomials of the modular system $\mathfrak{M}$ form a *residue class* and as all differ from each other merely by a linear function of the fundamental system of $\mathfrak{M}$, it follows that in our group considerations and work with congruences we can represent a residue class by any one residue belonging to it and chosen to represent it. This *representative residue*, which is usually designated by f, shall always be chosen in such a manner that its degree is less than that of ψ, which is always possible. Whenever it is feasible a residue so chosen to represent a given class may be replaced by some other residue belonging to the same class and therefore congruent to the first one modulo $\mathfrak{M}$, but when this is done the fact will be stated. The *norm* of $\mathfrak{M}$, written $N(\mathfrak{M})$, shall be defined as being equal to the number of residue classes belonging to $\mathfrak{M}$. This number evidently is equal to the number of residue classes belonging to m raised to a power equal to the degree of ψ, let us say $N(\mathfrak{M})=[N(m)]^{\kappa}$. When ψ is of degree 1 the residues must be of degree 0 and therefore are algebraic integers of Ω, which makes them identical with the residues of m. Hence when $\kappa=1$ it follows that the properties of the residue classes belonging to m are obtained from those belonging to $\mathfrak{M}$. Wolff and Ranum have studied this special case from the viewpoint of group theory.

Following Kronecker we shall say that the modular system $\mathfrak{M}$ is *contained* in the modular system $\mathfrak{M}'$ whenever it is possible to express every

element of the fundamental system of $\mathfrak{M}$ in terms of a linear form of the fundamental system of $\mathfrak{M}'$. Whenever there exists in addition to this a third modular system $\mathfrak{M}''$ such that any linear form contained in $\mathfrak{M}'$ (that is a linear form of the fundamental system of $\mathfrak{M}'$) when multiplied into any linear form contained in $\mathfrak{M}''$ always gives a linear form contained in $\mathfrak{M}$ we shall say that $\mathfrak{M}'$ is a *modular factor* of $\mathfrak{M}$, $\mathfrak{M}''$ is the *complementary factor* of $\mathfrak{M}'$, and that $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ is *equivalent* to the product of these modular systems. When speaking of modular factors we may drop the word modular. A modular system of the form $\mathfrak{P}=(\xi,\mathfrak{p})$ where $\mathfrak{p}$ is a prime ideal in Ω and ξ is irreducible modulo $\mathfrak{p}$ is defined as an *absolute prime modular system*. It may be remarked here that in this paper we consider only modular systems that contain $\mathfrak{M}$. Let us read = equivalent and make use of the following modular relation, true of any Kronecker modular system[20]) that

$$(M, M_1, M_2, \ldots, M_t) = (M'M'', M_1, \ldots, M_t) = (M', M_1, \ldots, M_t)(M'', M_1, \ldots, M_t)$$

whenever M is congruent to $M'M''$ modulo $(M_1, M_2, \ldots, M_t)$ and M' and M'' are relatively prime with respect to the same modular system. Here *relatively prime* means that there exists no modular system containing $(M_1, \ldots, M_t)$ that contains both M' and M'', excepting the unit system (1). From this it follows directly that

$$\mathfrak{M} = (\psi, \mathfrak{m}) = (\psi, \mathfrak{p}_1^{\alpha_1})(\psi, \mathfrak{p}_2^{\alpha_2}) \ldots . (\psi, \mathfrak{p}_r^{\alpha_r})$$

where $\mathfrak{m}=\mathfrak{m}'\mathfrak{m}''=\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\ldots\mathfrak{p}_i^{\alpha_i}\ldots\mathfrak{p}_r^{\alpha_r}$ when factored into its prime ideal factors. The ideals $\mathfrak{m}'$ and $\mathfrak{m}''$ always are relatively prime so that $\mathfrak{p}_i^{\alpha_i}, i \leqq r'$, divides $\mathfrak{m}'$, while $\mathfrak{p}_i^{\alpha_i}$, $r' < i \leqq r$, divides $\mathfrak{m}''$. Moreover

$$(\psi, \mathfrak{p}_i^{\alpha_i}) = (\psi_{1_i}, \mathfrak{p}_i^{\alpha_i})(\psi_{2_i}, \mathfrak{p}_i^{\alpha_i}) \ldots (\psi_{j_i}, \mathfrak{p}_i^{\alpha_i}) \ldots (\psi_{s_i}, \mathfrak{p}_i^{\alpha_i})$$

where $\psi \equiv \psi_{1_i}\psi_{2_i}\ldots\psi_{j_i}\ldots\psi_{s_i}$, mod $\mathfrak{p}_i^{\alpha_i}$, each ψ_{j_i} being of the highest pos-

[20]) König, Algebraische Grössen, p. 356: Hensel, Crelle, v. 118 (1897), p. 240.

sible degree so as to be contained in but one absolute prime system, and that one different from the absolute prime system containing any other ψ_{j_i}. The above relations we shall usually write in the form $\mathfrak{M}=\mathfrak{N}_1\mathfrak{N}_2\ldots\mathfrak{N}_i\ldots\mathfrak{N}_r$, where $\mathfrak{N}_i=(\psi,\mathfrak{p}_i^{\sigma_i})$ and furthermore $\mathfrak{N}_i=\mathfrak{Q}_{1_i}\mathfrak{Q}_{2_i}\ldots\mathfrak{Q}_{j_i}\ldots\mathfrak{Q}_{s_i}$, where $\mathfrak{Q}_{j_i}=(\psi_{j_i},\mathfrak{p}_i^{\sigma_i})$. Hence we have the relation

$$\mathfrak{M} = \mathfrak{Q}_{1_1}\mathfrak{Q}_{2_1}\ldots\mathfrak{Q}_{j_i}\ldots\mathfrak{Q}_{s_r}, \qquad i=1,2,\ldots,r;\ j_i=1_i,2_i,\ldots,s_i.$$

A modular system having the properties of the system $\mathfrak{Q}_{j_i}$ we shall define as an *irreducible modular system*. The absolute prime modular system containing $\mathfrak{Q}_{j_i}$ we shall designate by $\mathfrak{P}_{j_i}=(\xi_{j_i},\mathfrak{p}_i)$. Since no two of the irreducible modular systems containing $\mathfrak{M}$ are contained in the same absolute prime modular system it follows that they are all relatively prime to each other. Hensel has called them *einfache Modulsysteme* and proven that any modular system in one unknown can be factored in one and only one way so as to be represented by an equivalent product of irreducible modular systems. Such an irreducible modular system does not, in general, have as a modular factor the absolute prime modular system containing it, as has already been observed by Hensel, König, and others. Every irreducible modular system is of the form $\mathfrak{Q}_{j_i}=(\psi_{j_i},\mathfrak{p}_i^{\sigma_i})$, where $\psi_{j_i}\equiv\xi_{j_i}^{\varepsilon_{j_i}}$ modulo $\mathfrak{p}_i$, ξ_{j_i} being irreducible modulo $\mathfrak{p}_i$. This follows directly from the definition of an irreducible modular system as well as from a theorem first stated by Schönemann[21] for the rational realm which, by exactly the same proof, can be extended to any realm Ω. This theorem states that if any polynomial taken modulo $\mathfrak{p}$ can be broken up into n and no more factors relatively prime to another, then every polynomial that reduces to this given polynomial modulo $\mathfrak{p}$, must modulo $\mathfrak{p}^{\alpha}$ be fac-

[21]) Schönemann, Crelle, v.32 (1846), pp. 93ff.

torable into n factors and no more, all of them relatively prime to each other, mod $\mathfrak{p}^{\alpha}$. The concept of a prime modular system as given by König we shall not use, but the other definitions are in exact accord with those given in his book on pages 351-361.

Whenever a polynomial f belonging to the residue system of $\mathfrak{M}$ can be written as a linear form of the fundamental system of another modular system $\mathfrak{M}''$ it is of course congruent to 0 modulo $\mathfrak{M}''$ and is said to be contained in that modular system. When $\mathfrak{M}''$ happens to be a modular factor of $\mathfrak{M}$ we shall say that $\mathfrak{M}''$ is a *common factor* of f and $\mathfrak{M}$, and if there happen to be several their product is the *highest common divisor* of f and $\mathfrak{M}$. It may be observed here that every modular factor of $\mathfrak{M}$ must be the product of several irreducible modular factors of $\mathfrak{M}$ and that the term modular factor when applied to f is used in the sense of "contain" rather than that of "factor". We shall define f_1 and f_2 as relatively prime, mod $\mathfrak{m}$, if there exists no modular system containing f_1, f_2, and $\mathfrak{m}$ outside of the unit system (1). Similarly f is prime to $\mathfrak{M}$ if there exists no modular system besides unity that contains both f and $\mathfrak{M}$. The total number of residues prime to $\mathfrak{M}$ we shall define as the *totient* of $\mathfrak{M}$ and designate by $\varphi(\mathfrak{M})$. It may and in fact does frequently happen that there exists a modular system $\mathfrak{M}''$ not a modular factor of $\mathfrak{M}$ that contains both f and $\mathfrak{M}$. In this case f cannot be prime to $\mathfrak{M}$ nor has it a highest common divisor with $\mathfrak{M}$ according to the preceding definitions. Whenever this occurs we shall say that f and $\mathfrak{M}$ have the *hidden factor* $\mathfrak{M}''$ in common, where the hidden factor is not at all a modular factor of $\mathfrak{M}$ according to definition but merely a convenient term to express the relation existing between f and $\mathfrak{M}$. As an illustration we may

cite the residue x^3+4x^2+x belonging to the modular system $(x^4+5x^3+2x^2+7x,9)=(x^2+4x+7,9)(x+1,9)(x,9)$. The residue is prime to the modular factor $(x+1,9)$ and contains the common divisor $(x,9)$ with the modular system. While it is not contained in the system $(x^2+4x+7,9)$ it is not prime to this system since it is contained in the system $(x^2+x+1,3)$, which contains the former system. Hence $(x^2+x+1,3)$ is a hidden factor common to the residue and the modular system. When all the coefficients of f are contained in m we say m contains f. This can never happen for ψ excepting for the unit system since the coefficient of the highest power of ψ is 1 by assumption.

Whenever we shall speak of a necessary and sufficient condition that a set of residue classes belonging to $\mathfrak{M}$ form a group, we shall always mean the largest possible set, i.e. a set such that there exists no other residue class belonging to $\mathfrak{M}$ which when added to the set will cause the enlarged set also to form a group modulo $\mathfrak{M}$. Subsets of such a set may of course form subgroups of the group formed by the set. Similarly when we speak of groups of residue classes we shall mean groups belonging to such largest sets, unless the contrary is stated.

II. DETERMINATION OF CONDITIONS THAT A SET OF RESIDUE CLASSES FORM A GROUP.

We shall now proceed to determine the conditions under which a set of residue classes belonging to $\mathfrak{M}$ can form a group modulo $\mathfrak{M}$ by determining the conditions under which their representative residues form a group. Let us consider a set of these residues belonging to $\mathfrak{M}$ such that the set forms a group with respect to each of the modular systems $\mathfrak{N}_i$, $i=1,2,\ldots,r$, our set being understood to be such that it cannot be enlarged without violating this condition. It is at once evident that a

congruence holding for the modular system $\mathfrak{M}$ is also true for any system containing $\mathfrak{M}$. Conversely we know that a congruence true for every irreducible modular divisor of $\mathfrak{M}$ also holds modulo $\mathfrak{M}$[22]. Hence it follows that the product of any two residues of our set gives a third one of the set, mod $\mathfrak{M}$, for if this were not the case there would have to exist some modular system $\mathfrak{N}_i$ where the resulting residue is not an operator in the same group as the first two, which is contrary to assumptions. Furthermore if one residue of the set be multiplied by all of the set modulo $\mathfrak{M}$ we must get back the set. If this were not true at least one product would be repeated, let us say

$$f_1 f_2 \equiv f_1 f_3 \qquad \text{mod } \mathfrak{M},$$

from which it follows that

$$f_1 f_2 \equiv f_1 f_3 \qquad \text{mod } \mathfrak{N}_i, \quad i=1,2,\dots,r,$$

and since our residues form a group with respect to each one of these modular systems we must have

$$f_2 \equiv f_3 \qquad \text{mod } \mathfrak{N}_i, \quad i=1,2,\dots,r.$$

From this it follows at once that

$$f_2 \equiv f_3 \qquad \text{mod } \mathfrak{M},$$

which is contrary to hypothesis. Hence we get back the whole set. As the commutative and associative laws hold in the multiplication of polynomials we see that we have a sufficient condition that our set forms a group modulo $\mathfrak{M}$. That this condition is also necessary follows from the fact that if our set does not form a group with respect to at least one modular system $\mathfrak{N}_i$ we cannot get back the whole set modulo $\mathfrak{N}_i$ when we multiply the whole set by one of the set, and hence the same must

22) König, Algebraische Grössen, p. 355.

hold for modulus $\mathfrak{M}$. From this it follows that the condition is necessary. Since these same conditions must hold for the corresponding residue classes we have the following theorem:

THEOREM 1. *A necessary and sufficient condition that a set of residue classes taken with respect to the modular system* $\mathfrak{M}=\mathfrak{N}_1\mathfrak{N}_2\ldots\mathfrak{N}_r$ *form an abelian group is that they form a group with respect to each of the modular systems* $\mathfrak{N}_i$, $i=1,2,\ldots,r$.

Now that we have reduced the problem to one dealing with a modular system of the form $\mathfrak{N}$, we shall proceed to determine which residue classes or representative residues of the residue system belonging to $\mathfrak{N}$ can belong to a group. Every residue of this system belongs to one or the other of the following two divisions according to whether it does not or does possess a hidden factor in common with the modular system $\mathfrak{N}=(\mathfrak{w},\mathfrak{p}^{\alpha})=\mathfrak{N}'\mathfrak{N}''=\mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_j\cdots\mathfrak{Q}_s$:

I. Residues that contain the highest common divisor $\mathfrak{N}''$ in common with $\mathfrak{N}$ and are relatively prime to $\mathfrak{N}'$. For $\mathfrak{N}''=\mathfrak{N}$ this includes the 0 and for $\mathfrak{N}''=1$ the residues prime to $\mathfrak{N}$.

II. Residues that contain the highest common divisor $\mathfrak{N}''$ with $\mathfrak{N}$ and are contained in at least one absolute prime modular system containing $\mathfrak{N}'$.

Let us first take up class I and study the set of residues that contain the highest common divisor $\mathfrak{N}''$ in common with $\mathfrak{N}$ and are relatively prime to $\mathfrak{N}'$. The product of any two of this set must give a third one of the set, for if

$$f_1 f_2 \equiv f_3 \qquad \text{mod}\ \mathfrak{N}\,,$$

it necessarily follows that this congruence must also hold for every

modular system $\mathfrak{Q}_j$. For those values of $\mathfrak{Q}_j$ that are contained in $\mathfrak{N}''$ the left hand member is congruent to 0, hence the same is true for f_3, which therefore has the modular factor $\mathfrak{N}''$ in common with $\mathfrak{N}$. It remains to prove that f_3 is relatively prime to $\mathfrak{N}'$. If this is not the case there must exist some absolute prime modular system $\mathfrak{P}$ containing $\mathfrak{N}'$ for which our congruence must have its right hand member become congruent to 0 modulo $\mathfrak{P}$. Hence if $\mathfrak{P}=(\xi,\mathfrak{p})$ we can write

$$f_1 f_2 \equiv \zeta\xi \qquad \text{mod } \mathfrak{p},$$

so that either f_1 or f_2 must have the irreducible factor ξ of ψ in common with ψ modulo $\mathfrak{p}$. If $\zeta=0$ either f_1 or f_2 must be a linear form of the fundamental system of $\mathfrak{p}$. This is contrary to the assumption that both f_1 and f_2 are relatively prime to $\mathfrak{N}'$, from which it follows that f_3 must be relatively prime to $\mathfrak{N}'$. Consequently the product of two of the set gives another operator of the set, mod $\mathfrak{N}$. Moreover, when we multiply all operators of the set by one of the set we get back the whole set, mod $\mathfrak{N}$, for were this not true at least one product would be repeated. This would give a relation of the form

$$\text{(A)} \qquad f_1 f_2 \equiv f_1 f_3 \qquad \text{mod } \mathfrak{N},$$

and therefore

$$f_1(f_2 - f_3) \equiv \zeta\psi \qquad \text{mod } \mathfrak{p}^{\alpha}.$$

But $f_2 - f_3$ is of lower degree than ψ so that f_1 must contain a factor of ψ, mod $\mathfrak{p}^{\alpha}$, which is contrary to assumption. If $\zeta=0$ we either have f_1 as a linear form of the fundamental system of $\mathfrak{p}^{\alpha}$, or f_2 and f_3 are congruent modulo $\mathfrak{p}^{\alpha}$ and therefore modulo $\mathfrak{N}$. Since both cases are contrary to our assumptions no product can be repeated. As the commutative and associative laws of multiplication hold we see that our set forms a group,

so that every residue of class I belongs to a group. The 0 belongs to a group of order 1 formed by itself.

Let us now turn to class II and suppose that we have any residue of this class containing the highest common divisor $\mathfrak{N}''$ with $\mathfrak{N}$ to be contained in the absolute prime modular system $\mathfrak{P}_j$ of $\mathfrak{Q}_j$ where $\mathfrak{Q}_j$ contains $\mathfrak{N}'$. From this it follows that there exists an irreducible modular system $\mathfrak{Q}'=(\psi_j', \mathfrak{p}^{\alpha'})$, where $\alpha'<\alpha$ and ψ_j' is a factor of ψ_j, mod $\mathfrak{p}^{\alpha'}$, that contains the residue f under consideration. As a special case $\mathfrak{Q}'$ may be the absolute prime modular system $\mathfrak{P}_j$ itself. If f belongs to a group modulo $\mathfrak{N}$ it must necessarily belong to a group modulo $\mathfrak{Q}_j$. Consequently it must repeat itself for a certain power $\rho+1$ and for every power of the form $\rho^{\tau}+1$. Now let $\psi_j=\psi_j'$. Since f is a linear form of the fundamental system of $\mathfrak{Q}'$ we will have

$$f^2 = \psi_j^2\zeta^2 + 2\psi_j Q + Q^2$$
$$= \zeta'\psi_j + Q^2$$

where Q represents a linear form of the fundamental system of $\mathfrak{p}^{\alpha'}$. In a similar manner we have

$$f^{\tau} = \zeta''\psi_j + Q^{\tau}$$

and therefore

$$f^{\tau} \equiv 0 \qquad \text{mod } (\psi_j, Q^{\tau}).$$

As soon as we have a value of τ large enough so that $\tau\alpha'>\alpha$ this gives us the congruence

$$f^{\tau} \equiv 0 \qquad \text{mod } \mathfrak{Q}_j.$$

This means that every power of f greater than τ is congruent to 0 modulo $\mathfrak{Q}_j$, from which it follows that f cannot belong to a group modulo $\mathfrak{Q}_j$. When f happens to be contained in the modular system $\mathfrak{p}^{\alpha'}$ we need only

to raise it to its τ^{th} power, where $\tau\alpha' > \alpha$, to get a polynomial contained in $\mathfrak{p}^{\alpha}$. Hence f^{τ} and all succeeding powers of f are contained in $\mathfrak{N}$ and cannot belong to a group with respect to this modular system. Now let us suppose that ψ_j' is a divisor of ψ_j modulo $\mathfrak{p}^{\alpha'}$, and is not congruent to this polynomial. Moreover, suppose that f is not contained in $\mathfrak{p}$. With $\mathfrak{p}^{\alpha'}$ taken as modulus we can factor ψ_j into a product of powers of irreducible polynomials, at least one of which is contained to a lower power in ψ_j', mod $\mathfrak{p}^{\alpha'}$, than in ψ_j. Consequently f, which is contained in $\mathfrak{Q}' = (\psi_j', \mathfrak{p}^{\alpha'})$ but not in $\mathfrak{Q}_j$, must contain this particular factor to a lower power than ψ_j. We can now write

$$f = \psi_j'\zeta + R$$

where R is a linear form contained in $\mathfrak{p}^{\alpha'}$. Squaring we have

$$f^2 = (\psi_j'\zeta)^2 + 2\psi_j'\zeta R + R^2$$
$$= (\psi_j'\zeta)^2 + R'$$

where R' also is a linear form in $\mathfrak{p}^{\alpha'}$. Similarly for the τ^{th} power

$$f^{\tau} = (\psi_j'\zeta)^{\tau} + R''.$$

Continue this until τ assumes a value such that τ times the power of the irreducible factor of ψ_j' of which we have been treating modulo $\mathfrak{p}^{\alpha'}$ is a greater number than the power of this factor in ψ_j, mod $\mathfrak{p}^{\alpha'}$. Let ψ_j'' represent that divisor of ψ_j, mod $\mathfrak{p}^{\alpha'}$, that is equal to the product of ψ_j' and our special factor to a power sufficiently high so that it occurs to the same power in ψ_j and ψ_j'', mod $\mathfrak{p}^{\alpha'}$. It is evident that we have

$$f^{\tau} \equiv 0 \qquad \text{mod } (\psi_j'', \mathfrak{p}^{\alpha'}).$$

Since f itself is not contained in this modular system it cannot belong to a group modulo $(\psi_j'', \mathfrak{p}^{\alpha'})$ nor modulo $\mathfrak{N}$, since $(\psi_j'', \mathfrak{p}^{\alpha'})$ contains $\mathfrak{N}$. Con-

sequently no residue of class II can belong to a group and we have proven the theorem:

THEOREM 2. *A necessary and sufficient condition that a set of residue classes taken with respect to the modular system* $\mathfrak{N}=\mathfrak{N}'\mathfrak{N}''=\mathfrak{Q}_1\ldots\mathfrak{Q}_j\ldots\mathfrak{Q}_s$, $j=1,2,\ldots,s$, *form an abelian group is that the residues belonging to them comprise all the residues belonging to* $\mathfrak{N}$ *that have the greatest common divisor* $\mathfrak{N}''$ *with* $\mathfrak{N}$ *and are relatively prime to the modular system* $\mathfrak{N}'$.

As an example of a residue belonging to a group we may cite $2x^2+7x+5$ and its powers with respect to the modular system $(x^3+4x^2+2x+8,9)=(x+1,9)(x+5,9)(x+7,9)$. Here $\mathfrak{N}''=(x+1,9)(x+7,9)$ while the residue is relatively prime to $\mathfrak{N}'=(x+5,9)$. On the other hand the residue x^2+2x+1 taken modulo $(x^3+x,4)=(x^2+1,4)(x,4)$ does not belong to a group, for while it is not contained in the irreducible modular divisor $(x^2+1,4)$, it is contained in the absolute prime modular divisor $(x^2+1,2)$ containing the system $(x^2+1,4)$. By combining theorems 1 and 2 we immediately have a necessary and sufficient condition that a set of residue classes form a group modulo $\mathfrak{M}$. Writing $\mathfrak{M}=\mathfrak{N}_1\mathfrak{N}_2\ldots\mathfrak{N}_i\ldots\mathfrak{N}_r=\mathfrak{M}'\mathfrak{M}''$, where $\mathfrak{M}'=\mathfrak{N}'_1\mathfrak{N}'_2\ldots\mathfrak{N}'_i\ldots\mathfrak{N}'_r$, $\mathfrak{M}''=\mathfrak{N}''_1\mathfrak{N}''_2\ldots\mathfrak{N}''_i\ldots\mathfrak{N}''_r$, and $\mathfrak{N}_i=\mathfrak{N}'_i\mathfrak{N}''_i$ we have the theorem:

THEOREM 3. *A necessary and sufficient condition that a set of residue classes taken with respect to the modular system* $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ *form a group is that all residues belonging to these classes and only such residues have the greatest common divisor* $\mathfrak{M}''$ *in common with* $\mathfrak{M}$ *and are relatively prime to the modular system* $\mathfrak{M}'$.

This is a generalization of a theorem due to G.A. Miller stated in part one. Attention may be called to the fact that with respect to any

modular factor of $\mathfrak{M}$ contained in $\mathfrak{M}''$ the group formed by our residue classes is a group of order 1 since all the residues reduce to 0. The same group is obtained modulo $\mathfrak{M}$ whenever $\mathfrak{M}''=\mathfrak{M}$. For the case that $\mathfrak{M}''=1$ we have the residue classes prime to $\mathfrak{M}$ and $\varphi(\mathfrak{M})$ in number, so that we have the following corollary to theorem 8:

COROLLARY. *The set of residue classes comprising the totality of residues prime to the modular system* $\mathfrak{M}$ *form a group of order* $\varphi(\mathfrak{M})$. This group we shall define as the $\mathfrak{M}$ *group of totitives*. As mentioned in the historical sketch this group has been known for three quarters of a century for the case $\mathfrak{M}=m$ where m is a rational integer.

Let us now restrict ourselves to the absolute prime modular system $\mathfrak{M}=\mathfrak{P}=(\mathfrak{p},\mathfrak{b})$. We know that the congruence

$$A_0X^n + A_1X^{n-1} + \dots + A_n \equiv 0 \qquad \text{mod } \mathfrak{P},$$

where $A_0\neq 0$, the A's being polynomials, cannot be satisfied by more than n polynomials X[23]). All representative residues of $\mathfrak{P}$ excepting the 0 are prime to $\mathfrak{P}$. Let f be any one of the residues excepting 0. Since it belongs to the $\mathfrak{P}$ group of totitives it must repeat itself. Let τ designate its order. The polynomials $f, f^2, f^3, \dots, f^\tau=1$ are all incongruent. Let σ represent any one of the numbers $1,2,\dots,\tau$. Then

$$f^\tau \equiv 1 \qquad \text{mod } \mathfrak{P},$$

$$f^{\sigma\tau} \equiv 1 \qquad \text{mod } \mathfrak{P},$$

$$(f^\sigma)^\tau \equiv 1 \qquad \text{mod } \mathfrak{P},$$

$$(f^\sigma)^\tau - 1 \equiv 0 \qquad \text{mod } \mathfrak{P},$$

which gives a congruence of the form

$$X^\tau - 1 \equiv 0 \qquad \text{mod } \mathfrak{P},$$

23) König, Algebraische Grössen, p. 418.

and cannot have more than τ solutions. Since $f, f^2, f^3, \ldots, f^\tau$ satisfy this congruence it is evident that no other representative residue of $\mathfrak{P}$ can do so. Let δ be the order of f^σ, $\sigma=1,2,\ldots,\tau$. Now $\delta\sigma$ necessarily is a multiple of τ. If σ is prime to τ we have $\delta=\tau$, otherwise if ω is the greatest common divisor of τ and σ

$$(f^\sigma)^{\frac{\tau}{\omega}} \equiv (f^{\frac{\sigma}{\omega}})^\tau \equiv 1 \qquad \text{mod } \mathfrak{P},$$

so that f^σ is of lower order than f. As there are but $\varphi(\tau)$ integers of the set $1,2,\ldots,\tau$ that are prime to τ it follows that there are but $\varphi(\tau)$ residues belonging to our representative set modulo $\mathfrak{P}$ that are of order τ. Hence the $\mathfrak{P}$ group of totitives can have but one subgroup of order τ, where τ is the order of any operator of the group. Hence it follows that our group is cyclic. Since 0 is the only representative residue of $\mathfrak{P}$ that does not belong to this group we have its order equal to $N(\mathfrak{P})-1=p^{\lambda\nu}-1$, where $N(\mathfrak{P})=p^{\lambda\nu}$. Hence we have proven the theorem:

THEOREM 4. *All the residue classes of an absolute prime modular system $\mathfrak{P}$ with the exception of the one containing the 0 form a cyclic group of order $\varphi(\mathfrak{P}) = N(\mathfrak{P}) - 1 = p^{\lambda\nu} - 1$.*

This theorem was first proven by Serret for the special case where $\mathfrak{p}$ is a rational prime p and Ω is the rational realm.

III. DETERMINATION OF THE GENERATING SUBGROUPS OF A RESIDUE GROUP BELONGING TO $\mathfrak{M}$.

Now that we have determined a necessary and sufficient condition that a set of residues form a group modulo $\mathfrak{M}$ we shall proceed to establish a relation between the structure of such a group and the composition of the modular system to which it belongs. Let G denote a group of representative residues belonging to the modular system $\mathfrak{M}$, and let it

not be contained as a subgroup in a larger group of residues, mod $\mathfrak{M}$. This gives us the general case since any group belonging to $\mathfrak{M}$ can be put equal to G or to one of its subgroups. Let us put $\mathfrak{M}''=\mathfrak{N}_1''\mathfrak{N}_2''\ldots\mathfrak{N}_i''\ldots\mathfrak{N}_r''$ equal to the highest common divisor of every residue of G with $\mathfrak{M}$, so that every operator of the group is relatively prime to $\mathfrak{M}'=\mathfrak{N}_1'\mathfrak{N}_2'\ldots\mathfrak{N}_i'\ldots\mathfrak{N}_r'$, where $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ and $\mathfrak{N}_i=\mathfrak{N}_i'\mathfrak{N}_i''$. The residues of G when taken modulo $\mathfrak{N}_1$ form a group by theorem 1, which we shall designate by H_1. Similarly designate by H_i the various groups to which G reduces with respect to each of the modular systems $\mathfrak{N}_i$. If for any value of i we have $\mathfrak{N}_i=\mathfrak{N}_i''$, the group H_i is of order one an is represented by 0. If any group H_i is contained as a subgroup in a larger group modulo $\mathfrak{N}_i$, let the latter group be represented by H_i' and let it in turn not be contained in a larger group modulo $\mathfrak{N}_i$. For the present let us consider the set of groups H_i', $i=1,2,\ldots,r$, which we shall later prove to be identical with the set H_i. Since 0 cannot be contained in any group besides the one generated by itself we have $H_i'=H_i$ for the case where $\mathfrak{N}_i$ is a modular factor of the residues of G.

Now take any operator f_1 belonging to H_1' and any operator f_2 belonging to H_2'. We shall prove that there always exists a residue belonging to the modular system $\mathfrak{N}_1\mathfrak{N}_2$ such that it reduces to f_1 modulo $\mathfrak{N}_1$, and to f_2 modulo $\mathfrak{N}_2$. If there exists such a residue, which we shall designate by $f_{1,2}$ there must exist the congruences

$$f_{1,2}-f_1\equiv 0 \qquad \text{mod } \mathfrak{N}_1,$$

and

$$f_{1,2}-f_2\equiv 0 \qquad \text{mod } \mathfrak{N}_2.$$

Since f_1 and f_2 are both of lower degree in x than ψ is we can also write these congruences in the form

$$(1) \qquad f_{1,2} - f_1 \equiv 0 \qquad \text{mod } \mathfrak{p}_1^{\alpha_1},$$

and
$$(2) \qquad f_{1,2} - f_2 \equiv 0 \qquad \text{mod } \mathfrak{p}_2^{\alpha_2}.$$

There is a theorem stating that if $\mathfrak{b}$ and $\mathfrak{c}$ are any two ideals, there exists a number b in $\mathfrak{b}$ such that the ideal $\frac{b}{\mathfrak{b}} = \mathfrak{a}$ is relatively prime to the ideal $\mathfrak{c}$. Let the integer p' contained in $\mathfrak{p}_1^{\alpha_1}$ be such that $\frac{p'}{\mathfrak{p}_1^{\alpha_1}} = \mathfrak{a}$ is prime to $p_2^{\lambda_2 \alpha_2}$, the norm of $\mathfrak{p}_2^{\alpha_2}$. Since p' is contained in $\mathfrak{p}_1^{\alpha_1}$ it follows that there exists a polynomial contained in $\mathfrak{p}_1^{\alpha_1}$ which when added to the left hand member of (1) makes that member divisible by p', and therefore congruent to 0 modulo $\mathfrak{a}$. This fact we can indicate by the equation

$$(3) \qquad f_{1,2} - f_1 + p_1'\theta_1' + \dots + p_n'\theta_n' = a_1\theta_1 + \dots + a_n\theta_n$$

where $\mathfrak{a}=(a_1, a_2, \dots, a_n)$, $\mathfrak{p}_1^{\alpha_1}=(p_1', p_2', \dots, p_n')$, and $\mathfrak{p}_2^{\alpha_2}=(p_1'', p_2'', \dots, p_n'')$. Similarly we can add a linear form in the fundamental system of $\mathfrak{p}_2^{\alpha_2}$ to the left hand member of (2) so as to make that member divisible by $p_2^{\lambda_2 \alpha_2}$, equal to the norm of $\mathfrak{p}_2^{\alpha_2}$, which we can indicate by the equation

$$(4) \qquad f_{1,2} - f_2 + p_1''\theta_1'' + \dots + p_n''\theta_n'' = p_2^{\lambda_2 \alpha_2}\cdot\theta.$$

Eliminating the term $f_{1,2}$ from (3) and (4) we get

$$(5) \quad f_1 + a_1\theta_1 + \dots + a_n\theta_n - (p_1'\theta_1' + \dots + p_n'\theta_n') = f_2 + p_2^{\lambda_2 \alpha_2}\cdot - (p_1''\theta_1'' + \dots + p_n''\theta_n'').$$

Let us write $f_1' = f_1 - (p_1'\theta_1' + \dots + p_n'\theta_n')$ and $f_2' = f_2 - (p_1''\theta_1'' + \dots p_n''\theta_n'')$, so that we have

$$(6) \qquad f_1' + a_1\theta_1 + \dots + a_n\theta_n = f_2' + p_2^{\lambda_2 \alpha_2}\cdot\theta.$$

If we can prove the equation (6) to exist we have proven the existence of $f_{1,2}$, for this polynomial is equal to either member of (6). The equation exists if the equal powers of x that result on each side when the indicated operations are carried out have equal coefficients. That is, when the h^{th} power of x in f_1' has the coefficient A_h', that of f_2' has A_h'',

that of Θ has B_h, and that of the linear form $a_1\theta_1+\ldots+a_n\theta_n$ has $(a_1\lambda_1+\ldots+a_n\lambda_n)_h$, then we must have

(7) $$A'_h + (a_1\lambda_1 + \ldots + a_n\lambda_n)_h = A''_h + p_2^{\lambda_2\alpha_2}\cdot B_h,$$

which can be written

(8) $$A'_h - A''_h \equiv p_2^{\lambda_2\alpha_2}\cdot B_h \qquad \text{mod } \alpha.$$

In equations (1) to (8) we have treated $f_{1,2}$ as a determinate quantity, and the quantities $p'_1\theta'_1+\ldots+p'_n\theta'_n$ and $p''_1\theta''_1+\ldots+p''_n\theta''_n$ as depending upon this determinate value of $f_{1,2}$. We shall now assume $f_{1,2}$ to be indeterminate, while the linear forms $p'_1\theta'_1+\ldots+p'_n\theta'_n$ and $p''_1\theta''_1+\ldots+p''_n\theta''_n$ will be assigned definite values. Since f_1 and f_2 are known polynomials, so that the various coefficients A'_h and A''_h are known quantities. Consequently, in congruence (8) $A'_h-A''_h$, $p_2^{\lambda_2\alpha_2}$, and α are known. Since B_h is a coefficient of Θ it depends upon $f_{1,2}$ by (4) and therefore is an unknown. Confining ourselves to the domain of integrity of Ω we know that the product of a residue prime to α into the whole residue system of α gives back the whole system. Since α was chosen prime to $p_2^{\lambda_2\alpha_2}$ there must therefore exist a B_h that fulfils (8). Consequently $(a_1\lambda_1+\ldots+a_n\lambda_n)_h$ can be determined from (7). In this manner all coefficients of (6) and therefore of (5) can be obtained. But this gives us the polynomial $f_{1,2}$ which is equal to either member of (5). Equating it to the left hand member of (5) we have

$$f_{1,2} = f_1 + a_1\theta_1 + \ldots + a_n\theta_n - (p'_1\theta'_1 + \ldots + p'_n\theta'_n)$$

which, since $a_1\theta_1+\ldots+a_n\theta_n$ is divisible by p', reduces to the congruence

$$f_{1,2} \equiv f_1 \qquad \text{mod } \mathfrak{p}_1^{\alpha_1},$$

and therefore

$$f_{1,2} \equiv f_1 \qquad \text{mod } \mathfrak{N}_1,$$

which is congruence (1). Similarly when equating $f_{1,2}$ to the right member of (5) we have

$$f_{1,2} = f_2 + p_2^{\lambda_2 \alpha_2}\cdot\theta - (p_1''\theta_1'' + \dots + p_n''\theta_n''),$$

or
$$f_{1,2} \equiv f_2 \qquad \text{mod } \mathfrak{p}_2^{\alpha_2},$$

from which follows

$$f_{1,2} \equiv f_2 \qquad \text{mod } \mathfrak{N}_2,$$

which is congruence (2). No matter how $p_1'\theta_1'+\dots+p_n'\theta_n'$ and $p_1''\theta_1''+\dots+p_n''\theta_n''$ are chosen, we always get the same $f_{1,2}$ modulo $\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}$, and therefore modulo $\mathfrak{N}_1\mathfrak{N}_2$. For suppose that by assigning some other value to these linear forms we should obtain another polynomial $f'_{1,2}$. From (1) it follows that both $f_{1,2}-f_1$ and $f'_{1,2}-f_1$ and therefore $(f_{1,2}-f_1)-(f'_{1,2}-f_1)=$ $f_{1,2}-f'_{1,2}$ are all contained in $\mathfrak{p}_1^{\alpha_1}$. Similarly it follows from (2) that $f_{1,2}-f'_{1,2}$ is contained in $\mathfrak{p}_2^{\alpha_2}$. Hence $f_{1,2}-f'_{1,2}$ is contained in $\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}$ and we have

$$f_{1,2} \equiv f'_{1,2} \qquad \text{mod } \mathfrak{N}_1\mathfrak{N}_2,$$

which proves our statement. Hence the modular system $\mathfrak{N}_1\mathfrak{N}_2$ contains one and only one residue that is congruent to f_1 modulo $\mathfrak{N}_1$ and congruent to f_2 modulo $\mathfrak{N}_2$. It is evident that this same argument will hold if instead of restricting ourselves to H_1' and H_2' we take all residues of the modular systems $\mathfrak{N}_1$ and $\mathfrak{N}_2$.

We can continue this process by finding a residue $f_{1,2,3}$ belonging to the modular system $\mathfrak{N}_1\mathfrak{N}_2\mathfrak{N}_3$ such that taken modulo $\mathfrak{N}_1\mathfrak{N}_2$ it reduces to $f_{1,2}$ and when taken modulo $\mathfrak{N}_3$ it reduces to f_3, where f_3 is any residue belonging to H_3'. Repeating this we finally will have the relations

$$f \equiv f_i \qquad \text{mod } \mathfrak{N}_i, \quad i=1,2,\dots,r,$$

where the various f_i are r residues, one from each of the groups H_i',

that have been used to build up the residue f belonging to the modular system $\mathfrak{M}$ by the process described. No f could possibly reduce to two distinct sets of f_i residues belonging to the various groups H_i', and no two distinct f's belonging to $\mathfrak{M}$ can reduce to the same set of residues since these two would necessarily be congruent modulo $\mathfrak{M}$. Denote by G' the aggregate of residues f so obtained and belonging to the modular system $\mathfrak{M}$. By theorem 1 this set forms a group. Since there exists a (1,1) correspondence between the operators of this group and the total number of possible sets of residues, chosen one from each of the modular systems $\mathfrak{N}_i$, it follows that the order of G' is equal to the product of the orders of the groups H_i', $i=1,2,\ldots,r$. Repeating the same arguments with respect to the total residue systems of the moduli $\mathfrak{N}_i$ instead of restricting ourselves to the groups H_i' we have at once that the norm of $\mathfrak{M}$ is equal to the product of the norms of the moduli $\mathfrak{N}_i$, $i=1,2,\ldots,r$. This result has already been stated by Hensel[1]) and Landsberg[2]) for the case that m is a principal ideal in the rational realm.

Returning to the group G' we see that all of its operators contain in common with $\mathfrak{M}$ all the irreducible modular factors contained by the residues of G, since for these modular systems we have $H_i=H_i'$. Moreover since each H_i' contains the corresponding H_i as a subgroup it follows that G' contains G as a subgroup, for if this were not the case there would be instances in which two residues belonging to $\mathfrak{M}$ would reduce to the same set of residues f_i with respect to the various moduli $\mathfrak{N}_i$, and this is impossible. By assumption G is not contained in any larger group, mod $\mathfrak{M}$, so that it follows that $G'=G$, and $H_i'=H_i$ for all values of i. In the case where G is the $\mathfrak{M}$ group of totitives it follows that its or-

der is equal to the product of the orders of the groups of totitives of the various modular systems $\mathfrak{N}_i$, or the totient of $\mathfrak{M}$ is equal to the product of the totients of $\mathfrak{N}_1$, $\mathfrak{N}_2$, ..., $\mathfrak{N}_r$. This result has also been stated by Hensel[1]) for the rational realm.

We shall now prove that G is equal to the direct product of the groups H_1, H_2, ..., H_r. Let us choose that set of operators of G, in number equal to the order of H_1, that gives the group H_1 when taken modulo $\mathfrak{N}_1$, but which always gives the group of order 1 formed by the unit operator of the group H_i for each of the modular systems $\mathfrak{N}_i$, $i=2$, 3, ..., r. By theorem 1 this set forms a subgroup of G modulo $\mathfrak{M}$. Proceed to pick out in a similar manner $r-1$ more subgroups of G all of them possessing the same properties as the first, the h^{th} one, however, always reducing to H_h modulo $\mathfrak{N}_h$ and to the unit operators of all the other H_i for all the other modular systems $\mathfrak{N}_i$. Since no two operators of G reduce to the same set of residues with respect to the moduli $\mathfrak{N}_i$, $i=1,2,\ldots,r$, it follows from the manner of choosing our r subgroups that no two of them have any operator in common besides the identity. Now form the total number of different products that can be obtained modulo $\mathfrak{M}$ by multiplying together r residues modulo $\mathfrak{M}$, those in any given product being selected so that the product contains one and only one from each of the subgroups. No two of these products are congruent modulo $\mathfrak{M}$, for if this were the case and we had

$$f_1 f_2 \cdots f_r \equiv f_1' f_2' \cdots f_r' \qquad \text{mod } \mathfrak{M},$$

where f_h and f_h' belong to the same subgroup of G, while f_h and f_g, $h \neq g$, belong to different groups, we would also have

$$f_1 f_2 \cdots f_r \equiv f_1' f_2' \cdots f_r' \qquad \text{mod } \mathfrak{N}_i, \quad i=1,2,\ldots,r,$$

and since every one of the various f_h and f'_h residues, with the exception of f_i and f'_i, reduce to the unit operator of H_i, which we shall denote by u_i, with respect to the modular system $\mathfrak{N}_i$, we can write the last congruence in the form

$$u^{r-1}f_i \equiv u^{r-1}f'_i \qquad \text{mod } \mathfrak{N}_i, \; i=1,2,..,r.$$

Since u_i, f_i, and f'_i are all operators of H_i it follows that

$$f_i \equiv f'_i \qquad \text{mod } \mathfrak{N}_i, \; i=1,2,..,r,$$

and therefore

$$f_i \equiv f'_i \qquad \text{mod } \mathfrak{M},$$

for all values of i, which is contrary to assumption since these two residues are distinct operators of G. Since all of these products evidently belong to G and are distinct modulo $\mathfrak{M}$ it follows that they give us the entire group G, for the number of products is equal to the product of the orders of the various r subgroups, and this gives the order of G. Since there exists a simple isomorphism between the operators of of the i^{th} one of these subgroups and the operators of the group H_i, it follows that these subgroups are simply isomorphic, each to each, to the various groups H_i. Hence G is equal to the direct product of the groups H_i, $i=1,2,...,r$, where instead of the usual representative residues of the various H_i we may take as their representative residues the operators of the r subgroups of G. It follows at once that the same reasoning holds for a subgroup of G when compared with the subgroups of H_i to which this subgroup of G reduces modulo $\mathfrak{N}_i$, $i=1,2,...,r$. Hence we have proven the theorem:

THEOREM 5. *A group G of residue classes belonging to the modular system $\mathfrak{M}$ is equal to the direct product of the groups H_i formed by these*

classes when taken with respect to the modular systems $\mathfrak{N}_i$, $i=1,2,\ldots,r$, *where* $\mathfrak{M}=\mathfrak{N}_1\mathfrak{N}_2\cdots\mathfrak{N}_i\cdots\mathfrak{N}_r$.

We shall now proceed to consider the groups belonging to the modular system $\mathfrak{N}$, where $\mathfrak{N}=(\psi,\mathfrak{p}^\alpha)$. As before let $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_j, \ldots, \mathfrak{Q}_s$ represent the irreducible modular factors of $\mathfrak{N}$, their product being equal to $\mathfrak{N}$. Let $\mathfrak{Q}_j$ be of the form $(\psi_j,\mathfrak{p}^\alpha)$. From definition $\psi_j\equiv\xi_j^{\varepsilon_j}$, mod $\mathfrak{p}$, where the various ψ_j are all relatively prime modulo $\mathfrak{p}$. It is evident that the greatest common divisor that a residue belonging to $\mathfrak{Q}_j$ can have with $\mathfrak{Q}_j$ is either $\mathfrak{Q}_j$ itself or 1, so that the only residue groups formed modulo $\mathfrak{Q}_j$ are the $\mathfrak{Q}_j$ group of totitives and the one formed by 0. Let us consider any group H of residue classes belonging to $\mathfrak{N}$ whose representative residues have the greatest common divisor $\mathfrak{N}''$ with $\mathfrak{N}$, where $\mathfrak{N}=\mathfrak{N}'\mathfrak{N}''$, $\mathfrak{N}'=\mathfrak{Q}\ldots\mathfrak{Q}_{s'}$, and $\mathfrak{N}''=\mathfrak{Q}_{s'+1}\ldots\mathfrak{Q}_s$. We shall prove that H is the direct product of the residue groups K_j to which its operators reduce with respect to the modular systems $\mathfrak{Q}_j$, $j=1,2,\ldots,s$.

Let f_1 be any residue belonging to $\mathfrak{Q}_1$. For every residue f_1 belonging to $\mathfrak{Q}_1$ form a polynomial of the form $\psi_2\psi_3\ldots\psi_s\cdot f_1+u$, where u is the unit operator of H and hence is congruent to all of its own powers with respect to any one of the irreducible modular factors of $\mathfrak{N}$. No two of these polynomials are congruent modulo $\mathfrak{Q}_1$ since this would either involve the congruence of two distinct residues of $\mathfrak{Q}_1$ with respect to this modulus, or would require at least one of the ψ_j, $j=2,3,\ldots,s$, to be contained in the absolute prime modular factor containing $\mathfrak{Q}_1$. Since neither of these conditions holds our statement follows at once. Hence our polynomials are also incongruent modulo $\mathfrak{N}$. With respect to the prime modular systems $\mathfrak{Q}_j$, $j=2,3,\ldots,s$, every one of our polynomials evidently reduces to u.

For the present let us restrict ourselves to the group of residues whose operators are prime to $\mathfrak{Q}_1$. By theorem 1 this set also forms a group modulo $\mathfrak{N}$. Modulo $\mathfrak{Q}_1$ the restricted set of residues naturally forms the $\mathfrak{Q}_1$ group of totitives if we replace the usual representative residues of this group by those of our set. Let us denote this group by K_1'. Proceed in a similar manner to determine the groups K_j' belonging to the modular systems $\mathfrak{Q}_j$ for all values of j satisfying the relation $j \leqq s'$, all of these groups forming groups modulo $\mathfrak{N}$ and representing the totitive groups of their respective modular systems $\mathfrak{Q}_j$. It is evident that u forms the unit operator of each one of the groups K_j', $j \leqq s'$, since in setting up the system of polynomials $\psi_1\psi_2\ldots\psi_{j-1}\psi_{j+1}\ldots\psi_s \cdot f_j + u$, where f_j assumes all the values contained in the complete residue system of $\mathfrak{Q}_j$, f_j must also assume the value 0 which gives us the polynomial u which belongs to K_j', $j \leqq s'$, because it is prime to $\mathfrak{Q}_j$, $j \leqq s'$, by virtue of belonging to H. For all modular systems $\mathfrak{Q}_j$, $j > s'$, let the groups K_j' be represented as groups of order one whose operator is u which we shall take instead of the 0 to which u is congruent with respect to all these modular systems. It will be shown that the groups K_j' are identical with the groups K_j to which H reduces with respect to the various modular systems $\mathfrak{Q}_j$, and that H is equal to the direct product of these groups, j assuming all values.

Now let us consider all of the groups K_j', mod $\mathfrak{N}$. From their form it is evident that no two of the totality of operators belonging to these groups, excepting the u which belongs to each group, are congruent modulo $\mathfrak{N}$. Form the direct product of K_1' and K_2' modulo $\mathfrak{N}$. No two of the resulting polynomials are congruent modulo $\mathfrak{N}$, for if this did occur and we had

(9) $(\psi_1\psi_3\ldots\psi_s \cdot f_2'+u)(\psi_2\psi_3\ldots\psi_s \cdot f_1'+u) \equiv (\psi_1\psi_3\ldots\psi_s \cdot f_2''+u)(\psi_2\psi_3\ldots\psi_s \cdot f_1''+u)$ mod $\mathfrak{N}$,

where f_1' and f_1'' are distinct residues of $\mathfrak{Q}_1$ and f_2' and f_2'' are distinct residues of $\mathfrak{Q}_2$, it would follow that

$$\psi\cdot f_1' f_2'\cdot\psi_3\ldots\psi + \psi_3\ldots\psi_s(\psi_2 f_1' + \psi_1 f_2') + u \equiv \psi\cdot f_1'' f_2''\cdot\psi_3\ldots\psi_s + \psi_3\ldots\psi\ (\psi_1 f_2'' + \psi_2 f_1'') + u \qquad \text{mod } \mathfrak{N},$$

which reduces to

$$\psi_3\ldots\psi_s[\psi_1(f_2'-f_2'') + \psi\ (f_1'-f_1'')] \equiv 0 \qquad \text{mod } \mathfrak{N}.$$

Since f_1' and f_1'' are representative residues of $\mathfrak{Q}_1=(\psi_1,\mathfrak{p}^\alpha)$ it follows that $f_1'-f_1''$ is of a lower degree in x than ψ_1. Similarly $f_2'-f_2''$ is of lower degree than ψ_2. Hence the left hand member of the congruence is of lower degree than ψ in x and it follows that

$$\psi_3\ldots\psi_s[\psi_1(f_2'-f_2'') + \psi_2(f_1'-f_1'')] \equiv 0 \qquad \text{mod } \mathfrak{p}^\alpha.$$

Since $\mathfrak{p}$ is relatively prime to $\psi_3\ldots\psi_s$ we have

$$\psi_1(f_2'-f_2'') \equiv \psi_2(f_1''-f_1') \qquad \text{mod } \mathfrak{p}^\alpha,$$

and as ψ_1 and ψ_2 are relatively prime modulo $\mathfrak{p}^\alpha$ it follows that ψ_1 must be a factor of $f_1''-f_1'$, mod $\mathfrak{p}^\alpha$, and in a similar manner ψ_2 a factor of $f_2'-f_2''$, which is impossible since in both cases the ψ is of a higher degree in x than the polynomial of which it is to be a factor. Hence (9) cannot exist. By multiplying the polynomials obtained from the direct product of K_1' and K_2' into the polynomials forming the operators of K_3', we will find that the number of products obtained modulo $\mathfrak{N}$ is equal to the product of the orders of the groups K_1', K_2', and K_3'. By continuing this we find that the number of incongruent polynomials obtained modulo $\mathfrak{N}$ from the direct product of the groups K_j', $j=1,2,\ldots,s$, is equal to the product of the orders of these groups.

It is evident that all of these products belong to H, for each is of the form

$$(10)\quad (\psi_2\psi_3\ldots\psi_s\cdot f_1+u)(\psi_1\psi_3\ldots\psi_s\cdot f_2+u)\ldots(\psi_1\ldots\psi_{s'-1}\psi_{s'+1}\ldots\psi_s\cdot f_{s'}+u)\cdot u^{s''}$$

where the first factor belongs to K_1', the j^{th} to K_j', etc. For all modular systems where $j \overline{<} s'$ is satisfied the form (10) reduces to

$$(\psi_1 \ldots \psi_{j-1}\psi_{j+1} \ldots \psi_s \cdot f_j + u)u^{s-1} \equiv (\psi_1 \ldots \psi_{j-1}\psi_{j+1} \ldots \psi_s \cdot f_j + u) \bmod \mathfrak{Q}_j, j \overline{<} s',$$

an operator of K_j'. Consequently it follows that every form (10) is prime to every modular system $\mathfrak{Q}_j$, $j \overline{<} s'$, and therefore is relatively prime to $\mathfrak{N}'$, the product of these systems. On the other hand whenever we have a modular system $\mathfrak{Q}_j$, $j > s'$, every form (10) reduces to the form $u^s \equiv u \equiv 0$ since u is contained in each of these systems by virtue of belonging to H. Hence the forms (10) are contained in $\mathfrak{N}''$. From this it follows that every form (10) is an operator of H. Moreover these forms include all operators of H because every operator of that group must reduce to the same set of residues with respect to the various irreducible modular divisors of $\mathfrak{N}$ as one of these forms, from which follows the congruence of these two polynomials modulo $\mathfrak{N}$. Since the groups K_j', $j > s'$, contain only the operator u, which is also contained in the product of the groups K_1', K_2', ..., $K_{s'}'$, it follows that H is equal to the direct product of the groups K_j', $j \overline{<} s'$, and that for all values of j we have $K_j = K_j'$. This gives us the theorem:

THEOREM 6. *A group of residue classes belonging to the modular system $\mathfrak{N}$ is equal to the direct product of the groups formed by these residue classes when they are taken with respect to each of the various irreducible modular divisors of $\mathfrak{N}$ to which the residues they contain are relatively prime.*

This theorem is a generalization of the second theorem due to G.A. Miller stated in part one. By combining it with theorem 5 we have the complete generalization for the type of modular system discussed in this article. This gives us:

THEOREM 7. *A group of residue classes belonging to the modular system $\mathfrak{M}$ is equal to the direct product of the groups formed by these residue classes when they are taken with respect to each of the various irreducible modular divisors of $\mathfrak{M}$ to which the residues they contain are relatively prime.*

Our problem has now been reduced to the case of groups belonging to an irreducible modular system. We shall not take up the determination of the base and invariants of such a group on account of the difficulties inherent to the problem. It has been completely solved by Ranum for the modulus m in the quadratic realm Ω[13]) and partially for the modulus m in any realm Ω by Wolff[14]). Consequently we shall not take up the study of isomorphisms existing between any two groups belonging to any two given modular systems. The order of a group of residue classes will be treated in the next section with related considerations in number theory. We shall close this section with the following theorem whose proof follows directly from the facts that any modular system containing $\mathfrak{M}$ is itself the direct product of irreducible modular systems each of which contains one of the irreducible modular systems of which $\mathfrak{M}$ is the direct product, and that the group of totitives belonging to an irreducible modular system contains as a subgroup the group of totitives of every modular system that contains the first system. The first of these statements is self-evident, while the second follows from the fact that every quotient group of an abelian group is also a subgroup of this group. Hence we have:

THEOREM 8. *The group of totitives belonging to the modular system $\mathfrak{M}$ contains as a subgroup any group of residue classes belonging to $\mathfrak{M}$ or to any modular system containing $\mathfrak{M}$.*

IV. GENERALIZATION OF SOME WELLKNOWN THEOREMS IN NUMBER THEORY.

The results stated in the preceding theorems give rise at once to a number of generalizations of some very well-known theorems in number theory. To begin with, the fact that the representative residues prime to any modular system $\mathfrak{M}$ form a group of order $\varphi(\mathfrak{M})$ gives us at once the following generalization of Fermat's theorem:

THEOREM 9. *Whenever f is a residue of the modular system $\mathfrak{M}$ that is prime to $\mathfrak{M}$, then we have the relation $f^{\varphi(\mathfrak{M})} \equiv 1$, mod $\mathfrak{M}$.*

When we multiply the complete set of representative residues of the modular system $\mathfrak{M}$ into a residue prime to that system we must get back the whole system, for if this were not the case and the products $f_1 f_2$ and $f_1 f_3$ were congruent, f_1 being prime to $\mathfrak{M}$, we would have $f_1(f_2-f_3)$ contained in $\mathfrak{M}$, from which it would follow that f_2 and f_3 are congruent modulo $\mathfrak{M}$ by the same reasoning as was used in the case of congruence (A) in the proof of theorem 2. But this is contrary to assumptions so that we have:

THEOREM 10. *When the complete residue system of the modular system $\mathfrak{M}$ is multiplied by a residue prime to this modular system we get back the whole system.*

The well-known corollary of this theorem concerning the reduced residue system follows at once from the group property of the residues prime to $\mathfrak{M}$.

From group theory we know that the product of all the operators of a cyclic group of even order gives the operator of order 2. The cyclic $\mathfrak{P}$ group of totitives mentioned in theorem 4 has the operator -1 of order 2 and is therefore of even order. Hence we have the following generalization of Wilson's theorem:

THEOREM 11. *If $\mathfrak{P}$ is an absolute prime modular system, and f_1, f_2, ..., $f_{\varphi(\mathfrak{P})}$ is a complete system of residues prime to this modular system, then*

$$f_1 \cdot f_2 \cdot \ldots \ldots \cdot f_{\varphi(\mathfrak{P})} + 1 \equiv 0 \qquad \text{mod } \mathfrak{P}.$$

In proving theorem 5 we noticed that the norm of $\mathfrak{M}$ equals the product of the norms of its modular factors $\mathfrak{N}_i$, $i=1,2,\ldots,r$. Let us now take the complete residue systems of the modular systems $\mathfrak{Q}_j$, $j=1,2,\ldots,s$, whose product gives $\mathfrak{N}$, and replace the usual representative residues in every case by residues in the same general form as the residues belonging to the groups K_j' and used in proving theorem 6. By repeating the same line of reasoning as was used in that proof we can show that the number of products obtained modulo $\mathfrak{N}$ by multiplying together the different possible sets of s residues, each chosen so that one residue in each product is obtained from one of the different residue systems, is equal to the product of the norms of these modular systems $\mathfrak{Q}_j$. Moreover these products form a complete set of residues modulo $\mathfrak{N}$, for any residue of $\mathfrak{N}$ when taken with respect to the various moduli $\mathfrak{Q}_j$ will reduce to the same set of residues as one of these products, from which follows the congruence of these two residues modulo $\mathfrak{N}$. Combining this fact with the results obtained in the proof of theorem 5 we have the theorem:

THEOREM 12. *The norm of the modular system $\mathfrak{M}$ is equal to the product of the norms of its irreducible modular divisors.*

Let $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$ be any two irreducible modular divisors of $\mathfrak{M}$. It is evident from the proof of the preceding theorem that we can always choose one and only one residue of $\mathfrak{M}$ such that it is congruent to a given residue f_1 modulo $\mathfrak{Q}_1$, to a given residue f_2 modulo $\mathfrak{Q}_2$, and to 0 for any other ir-

reducible modular divisor of $\mathfrak{M}$. By allowing f_1 and f_2 to assume all values of their respective residue systems we get $N(\mathfrak{Q}_1)N(\mathfrak{Q}_2)$ incongruent residues of $\mathfrak{M}$. Moreover we know that these are the only residues belonging to a complete system of residues of $\mathfrak{M}$ that fulfil these conditions. It follows at once that our $N(\mathfrak{Q}_1)N(\mathfrak{Q}_2)$ residues are also incongruent modulo $\mathfrak{Q}_1\mathfrak{Q}_2$, for if $f_1 \equiv f_2$, mod $\mathfrak{Q}_1\mathfrak{Q}_2$, it follows that f_1 and f_2 are congruent with respect to every irreducible modular divisor of $\mathfrak{M}$, and therefore are congruent modulo $\mathfrak{M}$, which is contrary to assumptions. Since this set of residues must evidently contain the complete residue of $\mathfrak{Q}_1\mathfrak{Q}_2$, it follows that $N(\mathfrak{Q}_1\mathfrak{Q}_2)=N(\mathfrak{Q}_1)N(\mathfrak{Q}_2)$. This argument can be repeated by substituting for $\mathfrak{Q}_1$ and $\mathfrak{Q}_2$ any two modular factors of $\mathfrak{M}$ having no modular factor of $\mathfrak{M}$ in common. Hence we have proven the theorem:

THEOREM 13. *The product of the norms of any two relatively prime modular factors of $\mathfrak{M}$ is equal to the norm of their product.*

If we let $\mathfrak{M}'$ and $\mathfrak{M}''$ be any two complementary modular factors of $\mathfrak{M}$, it follows by the same reasoning as in the proofs of the preceding theorems that the total number of residues in $\mathfrak{M}$ that contain the modular factor $\mathfrak{M}''$ in common with $\mathfrak{M}$ is equal to the product of the norms of the irreducible modular factors of $\mathfrak{M}'$, or $N(\mathfrak{M}')$ by theorem 13. Hence we have:

THEOREM 14. *There are in a complete residue system of the modular system $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ exactly $N(\mathfrak{M}')$ residues divisible by the modular factor $\mathfrak{M}''$.*

As we have seen there always belongs a residue f to $\mathfrak{M}$ that will reduce to any given set of residues f_{j_i} with respect to the various irreducible modular factors $\mathfrak{Q}_{j_i}$ of $\mathfrak{M}$, and this f can be replaced in every congruence by any residue belonging to the same residue class, mod $\mathfrak{M}$. This gives us the theorem:

THEOREM 15. *If the modular system* $\mathfrak{M}$ *is the product of the irreducible modular systems* $\mathfrak{Q}_{j_i}$, $i=1,2,\ldots,r$, $j_i=1_i,2_i,\ldots,s_i$, *and if* $f_{1_1},\ldots, f_{j_i},\ldots, f_{s_r}$ *be any polynomials, there exist polynomials,* f, *such that*

$$f \equiv f_{j_i} \qquad \mathrm{mod}\ \mathfrak{Q}_{j_i},$$

and all of these polynomials are congruent each to each modulo $\mathfrak{M}$.

It is evident that this theorem also holds if instead of breaking $\mathfrak{M}$ up into its irreducible factors we were to break it up into any number of its modular factors, all of them relatively prime and each one being a product of irreducible factors of $\mathfrak{M}$. It is in this form that the special case for the ideal $\mathfrak{m}$, i.e. when $\kappa=1$ in ψ, is úsually stated.[24] This property of the residue classes of a modular system $\mathfrak{M}$ in the realm $(x,1)$ was already noticed by Landsberg[2], although he does not seem to have noticed any of the group properties connected with this fact.

The $\mathfrak{M}$ group of totitives is necessarily composed of residue classes whose residues are prime to every irreducible modular factor of $\mathfrak{M}$. From this it follows by means of the proofs of theorems 5, 6, and 7 that the groups to which this group reduces with respect to the irreducible modular factors of $\mathfrak{M}$ are the groups of totitives of these divisors. Since $\varphi(\mathfrak{M})$ is equal to the order of our group it follows from theorem 7 that we have:

THEOREM 16. *The value of the totient of a modular system* $\mathfrak{M}$ *is equal to the products of the totients of its irreducible modular divisors, or*

$$\varphi(\mathfrak{M}) = \varphi(\mathfrak{Q}_{1_1})\varphi(\mathfrak{Q}_{2_1})\ldots\varphi(\mathfrak{Q}_{j_i})\ldots\varphi(\mathfrak{Q}_{s_r})$$

where $\mathfrak{Q}_{s_r}$, $j_i=1_1,\ldots,j_i,\ldots,s_r$, *represent the irreducible modular factors of* $\mathfrak{M}$.

[24]) See Hilbert, Bericht über die Theorie der Algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker Vereinigung, v. IV, p. 28.

When $\kappa=1$ we have $s_i=1$ for all values of i and our function reduces to

$$\varphi(m) = \varphi(\mathfrak{p}_1^{\alpha_1})\varphi(\mathfrak{p}_2^{\alpha_2})\ldots\varphi(\mathfrak{p}_r^{\alpha_r})^{24}).$$

Let G be the largest possible group contained in the system of representative residues of $\mathfrak{M}$ such that the residues of G contain the greatest common divisor $\mathfrak{M}''$ in common with $\mathfrak{M}$, but are relatively prime to $\mathfrak{M}'$, where $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$. From theorem 7 the order of G is equal to $\varphi(\mathfrak{M}')$. Hence it follows that we have:

THEOREM 17. *The number of residues belonging to a complete residue system of $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ that contain with $\mathfrak{M}$ the greatest common divisor $\mathfrak{M}''$ and are relatively prime to $\mathfrak{M}'$ is equal to $\varphi(\mathfrak{M}')$.*

Let us now proceed to consider the solution of the congruence $f_1X\equiv f_2$, mod $\mathfrak{M}$, where f_2 is any residue belonging to $\mathfrak{M}$, while f_1 is any residue of $\mathfrak{M}$ that does not have a hidden factor in common with $\mathfrak{M}$. This restriction is made so as to avoid the difficulty connected with the factorization of a residue having a hidden factor in common with $\mathfrak{M}$. Since any solution X of the congruence, mod $\mathfrak{M}$, must also hold for all the irreducible factors $\mathfrak{Q}$ of $\mathfrak{M}$, we shall study the following possibilities that may occur with respect to any given $\mathfrak{Q}$:

1) Both f_1 and f_2 are prime to $\mathfrak{Q}$;

2) While f_1 is prime to $\mathfrak{Q}$, f_2 is contained in $\mathfrak{Q}$;

3) Both f_1 and f_2 are contained in $\mathfrak{Q}$;

4) While f_1 is prime to $\mathfrak{Q}$, f_2 has a hidden factor in common with $\mathfrak{Q}$;

5) While f_2 is prime to $\mathfrak{Q}$, f_1 is not.

The last possibility cannot occur, for it is evident that if the congruence is solvable the right hand side of the congruence must vanish whenever this is true of the left hand member. This gives us a

necessary condition for the solution of the congruence. If case 1) occurs, both f_1 and f_2 belong to the $\mathfrak{Q}$ group of totitives so that there can be but one value of X belonging to $\mathfrak{Q}$ that satisfies the congruence. Hence it follows that no matter how many incongruent values of X may satisfy our congruence modulo $\mathfrak{M}$, they must all reduce to the same value with respect to any irreducible modular divisor of $\mathfrak{M}$ to which f_1 and f_2 are both prime. In the second case we have a congruence of the form $f_1 \cdot X \equiv 0$, mod $\mathfrak{Q}$, so that X must be 0 because f_1 is prime to $\mathfrak{Q}$. Consequently there is but one value of X that satisfies our congruence with respect to any factor $\mathfrak{Q}$ of $\mathfrak{M}$ that belongs to the second class. In the third case we have $0 \cdot X \equiv 0$, mod $\mathfrak{Q}$, so that any one of the $N(\mathfrak{Q})$ values of the incongruent residues of $\mathfrak{Q}$ can be taken for X. Finally, for case 4) there can be, by theorem 10, but one value of X for any modulus $\mathfrak{Q}$ belonging to this class. Now the total number of solutions X, mod $\mathfrak{M}$, is equal to the total number of residue combinations possible by taking for each combination a residue from each of the various systems $\mathfrak{Q}$ contained in $\mathfrak{M}$, these residues being chosen only for such values of X as X can satisfy for the modulus $\mathfrak{Q}$ to which eachresidue belongs. This number is at once seen to be equal to $N(\mathfrak{M}'')$, where $\mathfrak{M}''$ is the greatest common divisor of f_1 and $\mathfrak{M}$. Hence we have the theorem:

THEOREM 13. *A necessary and sufficient condition that the congruence $f_1 X \equiv f_2$, mod $\mathfrak{M}$, be solvable, where f_1 and f_2 are any residues of $\mathfrak{M}$ excepting that f_1 and $\mathfrak{M}$ have no hidden factor in common; is that f_1 contains as a modular factor the highest common divisor $\mathfrak{M}''$ of f_1 and $\mathfrak{M}$. The number of solutions is equal to $N(\mathfrak{M}'')$.*

We shall now proceed to determine the order of the group of toti-

tives of an irreducible modular system. Since such a system is contained in only one absolutely prime modular system it follows that any polynomial that is prime to the one is prime to the other. Hence, the group of totitives of any modular system $\mathfrak{Q}$ will reduce to the group of totitives of any modular system containing $\mathfrak{Q}$ when taken modulo that system. Moreover the number of residues of $\mathfrak{Q}$ that reduce to any given residue of the second system, let us call it $\mathfrak{Q}'$, evidently always is the same, and must therefore be equal to the quotient of the norms of the two systems. Hence it follows that

$$\varphi(\mathfrak{Q}) = \frac{N(\mathfrak{Q})}{N(\mathfrak{Q}')}\cdot\varphi(\mathfrak{Q}').$$

By putting $\mathfrak{Q}=(\psi,\mathfrak{p}^{\alpha})$ and $\mathfrak{Q}'=(\psi',\mathfrak{p}^{\alpha'})$, where $\psi\equiv\xi^{\varepsilon}$, mod $\mathfrak{p}$, and $\psi'\equiv\xi^{\varepsilon'}$, mod $\mathfrak{p}$, where ξ is of degree ν, we have ψ and ψ' of degree $\nu\varepsilon$ and $\nu'\varepsilon'$ respectively. Remembering that $N(\mathfrak{p})=p^{\lambda}$, the above expression now reduces to

$$\varphi(\mathfrak{Q}) = \frac{p^{\lambda\alpha\varepsilon\nu}}{p^{\lambda\alpha'\varepsilon'\nu}}\cdot\varphi(\mathfrak{Q}') = p^{\lambda\nu(\alpha\varepsilon-\alpha'\varepsilon')}\cdot\varphi(\mathfrak{Q}').$$

In case $\mathfrak{Q}'=\mathfrak{P}$ is an absolute prime modular system we have $\nu'\varepsilon'=1$, while $N(\mathfrak{P})=p^{\lambda\nu}-1$ by theorem 4. Consequently we have

$$\varphi(\mathfrak{Q}) = p^{\lambda\nu(\alpha\varepsilon-1)}\cdot(p^{\lambda\nu}-1) = p^{\lambda\alpha\varepsilon\nu}[1 - \frac{1}{p^{\lambda\nu}}] = [N(\mathfrak{p}^{\alpha})]^{\nu\varepsilon}[1 - \frac{1}{[N(\mathfrak{p})]^{\nu}}].$$

or

$$\varphi(\mathfrak{Q}) = N(\mathfrak{Q})[1 - \frac{1}{N(\mathfrak{P})}]^{24)}.$$

Hence we have the theorem:

THEOREM 19. *The value of the totient of the irreducible modular system* $\mathfrak{Q}$ *is given by the expression* $\varphi(\mathfrak{Q}) = N(\mathfrak{Q})[1 - \frac{1}{N(\mathfrak{P})}]$, *where* $\mathfrak{P}$ *contains* $\mathfrak{Q}$.

Since an abelian group is equal to the direct product of its Sylow subgroups it follows that the group of totitives belonging to an irreducible modular system is equal to the direct product of two abelian groups

of orders $p^{\lambda\nu(\alpha\varepsilon-1)}$ and $p^{\lambda\nu}-1$ respectively, the latter group being cyclic by theorems 4 and 8.

Since the order of any group taken modulo $\mathfrak{M}$ and not contained in a larger group with respect to this modular system depends only upon properties stated in theorems 7 and 19, it follows at once that we have:

THEOREM 20. *The order of a group of residue classes belonging to the modular system $\mathfrak{M}=\mathfrak{M}'\mathfrak{M}''$ such that every polynomial contained in these classes has the greatest common divisor $\mathfrak{M}''$ with $\mathfrak{M}$ and is relatively prime to $\mathfrak{M}'$, the group not being contained in a larger group modulo $\mathfrak{M}$, is equal to $\varphi(\mathfrak{M}')$ where*

$$\varphi(\mathfrak{M}')=\prod_{i=1}^{i=r'}\prod_{j_i=1_i}^{j_i=s_i'} N(\mathfrak{Q}_{j_i})\left[1-\frac{1}{N(\mathfrak{P}_{j_i})}\right]=\prod_{i=1}^{i=r'}\prod_{j_i=1_i}^{j_i=s_i'} p_i^{\lambda_i\alpha_i\varepsilon_{j_i}\nu_{j_i}}\left(1-\frac{1}{p_i^{\lambda_i\nu_{j_i}}}\right).$$

If $\mathfrak{M}''=1$ we have at once the value of the totient of $\mathfrak{M}$, which could also have been determined directly from theorems 16 and 19:

THEOREM 21. *The value of the totient of any modular system $\mathfrak{M}$ is given by the expression:*

$$\varphi(\mathfrak{M}) = N(\mathfrak{M})\prod_{i=1}^{i=r}\prod_{j_i=1_i}^{j_i=s_i}\left[1-\frac{1}{N(\mathfrak{P}_{j_i})}\right]$$

When $\kappa=1$ we get $N(\mathfrak{M})=N(m)$, while $s_i=s_1$ for every value of i. Hence our expression will reduce to the well-known form

$$\varphi(m) = N(m)\left(1-\frac{1}{N(\mathfrak{p}_1)}\right)\left(1-\frac{1}{N(\mathfrak{p}_2)}\right)\ldots\left(1-\frac{1}{N(\mathfrak{p}_r)}\right).$$ [24]

VITA.

The writer was born in Chicago, Illinois, on March 21, 1890. He graduated from the grammar and high schools of that city and entered the University of Illinois in 1908. After receiving his A.B. degree in 1911 he kept on with his graduate work in mathematics, receiving the A.M. degree in 1912. The first year of his graduate work he was a scholar and the last two years a fellow in mathematics. He wishes to make use of this opportunity to express his thanks to the various members of the faculty under whom he has had the pleasure of studying during the last few years, especially to Prof. G.A. Miller and Dr. G. Wahlin to whose advice and suggestions he is very much indebted in the preparation of this thesis.